March 02, 2023

Share

Blockchain Security Monthly Recap of February: $56.88M lost in attacks

It's time for our monthly security report! According to Beosin EagleEye security risk monitoring, warning, and blocking platform, in February 2023, the number of various security incidents and the amount involved increased significantly compared with January 2023. In this month, more than 21 typical security incidents occurred and the total loss of various security incidents was about 56.88 million US dollars, which is up about 288% compared with last month.

There were eight security incidents this month, each of which suffered a loss of more than a million dollars, including MyAlgo (a loss of $9.2 million), Platypus Finance (a loss of $8.5 million), and Shata Capital (a loss of $5.1 million). About half of this month's losses came from attacks on individual users: the exploit of MyAlgo Wallet which pilfered over $9.2 million from 25 users. The number of NFT phishing scams increased a lot with a loss of NFT assets worth at least $20 million.

DeFi『11』Typical Security Incidents

No.1 On February 2, a Polygon-based project BonqDAO lost about $1,850,000 due to an attack.

No.2 On February 3, Orion Protocol was exploited by a reentrancy attack and suffered a loss of $3,020,000.

No.3 On February 4, SperaxUSD was attacked due to an error in its multi-sig wallet and the attacker minted 9.7 billion USDs for a profit of $310,000.

No.4 On February 8, LianGo suffered its compromised private key with a loss of $1,260,000.

No.5 On February 10, dForce was attacked and lost $3,700,000.

No.8 On February 21, Layer1 Kujira built on Cosmos was attacked and the loss was about $230,000.

No.9 On February 24, FEG Protocol, a multi-chain DeFi project, was attacked with a loss of $200,000. It suffered two attacks in May 2022 with a loss of $1,300,000 and $1,900,000 respectively.

No.10 On February 24, Shata Capital's upgraded smart contract was attacked and the attacker made a profit of $5,100,000.

No.11 On February 27, the smart contract of SwapX was attacked due to a missing authentication in its key function. Multiple tokens which give approvals to the contract were exploited with a total loss of $900,000.

NFT『3』Typical Security Incidents

No.1 On February 22, the smart contract of CryptoNinja World had a serious vulnerability that allowed anyone to burn any CryptoNinja NFT.

No. 2 On February 24, NFTCloud which is a platform that offers a suite of tools for Web3 builders was attacked with a loss of $80,000.

No. 3 There were several NFT phishing scams in February and many kinds of NFT assets including BAYC, Otherdeed, Doodles, Meebits, and mfters were stolen. The total loss was more than $20,000,000.

Wallet Security『1』Typical Security Incidents

No.1 From 19-21 February, MyAlgo, an Algorand wallet project, was attacked and there were 25 stolen users with a total loss of more than $9,200,000. The cause is still under investigation.

Rug Pull/Crypto Scam『2』Typical Security Incidents

No.1 On February 7, the contract of WOOF token had a backdoor and the contract deployer made a profit of $110,000 after a rug pull.

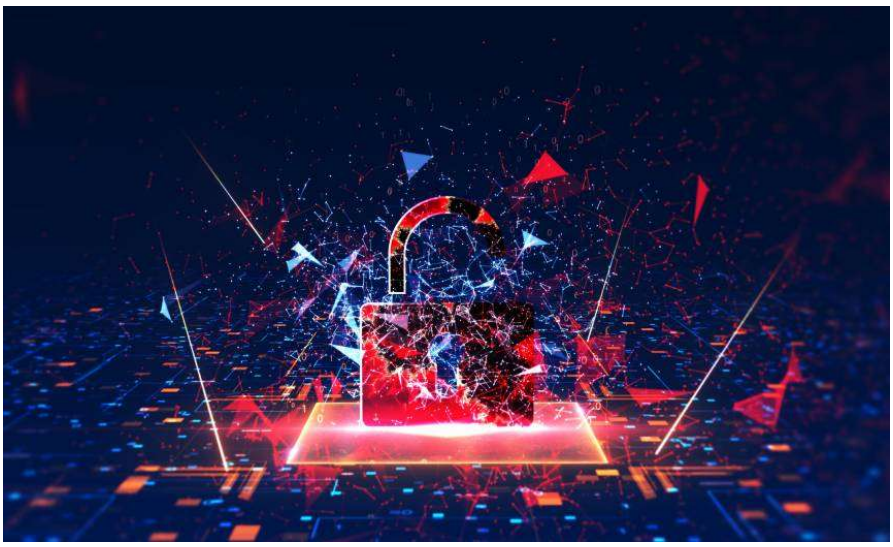
No.2 On February 21, Hope Finance, an Arbitrum-based project had a rug pull and the fraudster made a profit of about $1,800,000 and transferred the fund into Tornado Cash.

Crypto Crime『4』Typical Security Incidents

No.1 Australia police dismantled a Chinese-Australian money-laundering syndicate and seized assets worth more than $106 million

No.3 Eddy Alexandre, the CEO of a crypto trading platform EminiFX, pled guilty to $248M fraud scheme and faced 10 years in prison.

No.4 Forsage founders were indicted in $340M DeFi crypto scheme.



In view of the current new situation in the field of blockchain security, Beosin concludes:

Generally, in February 2023, the number of various security incidents and the amount involved increased significantly compared with January. The total loss of various security incidents was about 56.88 million US dollars, which is up about 288% compared with January.

There were more stolen funds recovered this month. Hackers returned all the $3.65 million they had stolen from dForce Network. Hackers suspected of attacking Platypus were arrested by French police. We can foresee that global cryptocurrency regulation is an inevitable trend, and expect more cases of stolen funds to be recovered in the future. About 50 percent of attacks in February were due to contract vulnerabilities. It is recommended that project teams complete professional smart contract audits before launching their projects. Moreover, users are advised to check projects' audit reports carefully before interacting with them to avoid asset loss.

Beosin is a leading global blockchain security company co-founded by several professors from world-renowned universities and there are 40+ PhDs in the team. It has offices in Singapore, South Korea, Japan and other 10+ countries. With the mission of "Securing Blockchain Ecosystem", Beosin provides "All-in-one" blockchain security solution covering Smart Contract Audit, Risk Monitoring & Alert, KYT/AML, and Crypto Tracing. Beosin has already audited more than 3000 smart contracts including famous Web3 projects PancakeSwap, Uniswap, DAI, OKSwap and all of them are monitored by Beosin EagleEye. The KYT AML are serving 100+ institutions including Binance.

About Us

Terms and Conditions

Privacy Policy

Channel Verification

Solution

Compliance

Smart Contract Security